IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

JERRON KNOX, on behalf of himself and on behalf of all persons similarly situated, Plaintiffs, v. TARGET CORPORATION, a Minnesota Corporation Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jerron Knox brings this action against Target Corporation (hereinafter "Defendant" or "Target) on behalf of himself and all others similarly situated. Plaintiff makes the following allegations upon information and belief, except as to allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF THE ACTION

1. Plaintiff Knox brings this class action Complaint against Target for failing to secure and safeguard its customers' personal financial data, including credit and debit card information and personal identification numbers (PINs), and personal information, including names, mailing addresses, telephone numbers, and email addresses.

2. In December 2013, it was reported that data thieves had stolen from Target the personal financial information of customers who had made purchases with the retailer from November 27, 2013, to December 15, 2013. Target stated initially that approximately 40 million customers were affected by the data theft.

3. On January 10, 2013, Target announced that, in addition to the financial information stolen from the retailer, the personal information – names, mailing addresses, phone numbers, and email addresses – of as many as 70 million Target customers had been stolen.

4. Plaintiff Knox made a purchase at a Target location in Charlotte, North Carolina on December 1, 2013, with his debit card.

5. On January 10, 2014, Plaintiff Knox received notification that an unauthorized user was attempting to access his email account.

6. On January 14, 2014, Plaintiff Knox became aware of a fraudulent and unauthorized purchase on his debit card.

7. As a direct result of the data breach, and Target's failure to adequately secure and safeguard its customers' personal financial data and personal information, Plaintiff and others similarly situated have had that information compromised and those persons have been injured financially.

PARTIES

8. Plaintiff Knox is a resident of Mecklenburg County, North Carolina.

9. Defendant Target is a Minnesota corporation, with its corporate headquarters located at 1000 Nicollet Mall, Minneapolis, Minnesota, 55403. Target is one of the largest retailers in the country with nearly 1,800 stores located across the United States. Forty-seven of Target's stores are located in North Carolina.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because the claims asserted herein arise under federal statute, the Federal Stored Communications Act, 18 U.S.C. § 2702. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §

1332(d)(2)(A) because this case is a class action in which the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interests and costs, and Plaintiff, as well as most members of the proposed class, are citizens of states different from the State of the Defendant.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 in that a substantial part of the events giving rise to the claims stated herein occurred in this judicial district.

FACTUAL ALLEGATIONS

A. The Target Data Breach

12. On December 18, 2013, Target's data breach was first reported by Brian Krebs on his internet blog. See Brian Krebs, *Sources: Target Investigating Data Breach*, KrebsonSecurity.com (Dec. 18 2013), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

13. Target did not make any attempt to warn victims of the data breach until December 19, 2013, when it released a statement on its website, confirming Brian Krebs' report of the data breach:

> Target today confirmed ***it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores.*** Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.
>
> "Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."
>
> ***Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013***. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other

> actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores, Target.com (Dec. 19, 2013), http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores (emphasis added). The information stolen by the data thieves included customers' personal identification numbers ("PINs"). See Amrita Jayakumar and Hayley Tsukayama, *Target breach: What you need to know*, Washingtonpost.com, http://www.washingtonpost.com/business/economy/target-breach-what-you-need-to-know/2014/01/10/669a5c9c-7a10-11e3-8963-b4b654bcc9b2_story.html.

14. On January 10, 2014, Target announced that, in addition to the financial data of 40 million customers, data thieves had also stolen "certain guest information." *Target Provides Update on Data Breach and Financial Performance*, Target.com (Jan. 10, 2014), http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance. Specifically, "the stolen information includes **names, mailing addresses, phone numbers or email addresses** for up to ***70 million individuals***." Id. (emphasis added).

15. In a January 12, 2014 interview with CNBC, Target Chairman and Chief Executive Officer Gregg Steinhafel stated that "clearly we are accountable and we are responsible." Becky Quick, *Target CEO defends 4-day wait to disclose massive data hack*, CNBC.com (Jan. 12, 2014), http://www.cnbc.com/id/101329300. In that same interview, Steinhafel stated that the breach occurred due to "malware [that] was installed on the company's point of sale registers" and that the company "confirmed" that the breach had occurred on December 15. Id.

B. Plaintiff Knox's Target Purchases and Subsequent Compromise of His Personal Financial Data and Information

16. Plaintiff Knox has a RushCard,[1] to which his paychecks from his employer, the American Red Cross, are deposited, and for which he uses to make his day-to-day purchases. Plaintiff Knox frequently made such purchases at Target locations.

17. On December 1, 2014, Plaintiff Knox made an in-store purchase at the 8830 Albemarle Road, Charlotte, North Carolina Target location using his RushCard.

18. On January 10, 2014, Plaintiff Knox received a notification from his email provider, Gmail, that someone in Huangshi, Hubei, China had attempted to use his password to access his email account.

19. On January 14, 2014, Plaintiff Knox received a "RushCard Alert" showing a low balance and indicating that someone had used his card information to make a purchase of $162.50 at a Wal-Mart in Houston, Texas. Knox immediately contacted the customer service department of RushCard. While RushCard was able to reverse the charges, Plaintiff was forced to request a new card and is currently awaiting its issuance. Until he receives the new card, he is unable to access funds in order to fund day-to-day expenses.

20. Plaintiff Knox has also contacted Target but was only given several numbers to call and ultimately told he could get free credit reporting for a period.

CLASS ACTION ALLEGATIONS

21. Plaintiff brings this action on his own behalf, and on behalf of all other persons similarly situated. Specifically, Plaintiff seeks to represent a Class defined as:

Nationwide Class:

[1] RushCard is a prepaid Visa debit card. See https://www.rushcard.com/home#PayYourOwnWay. RushCard allows for direct deposits of paychecks to be made on the cards. See https://www.rushcard.com/direct-deposit.

> All persons residing in the United States who made an in-store purchase at a Target store located in the United States using a debit or credit card during the period of November 27, 2013 to December 15, 2013.

North Carolina Subclass:

> All persons residing in North Carolina who made an in-store purchase at a Target store located in North Carolina using a debit or credit card during the period of November 27, 2013 to December 15, 2013.

Excluded from the Class are Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded from the Class is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

22. Members of the Class are so numerous that their individual joinder herein is impracticable. According to Target, personal and financial information was stolen from as many as 110 million customers across the United States. Moreover, the number of customers affected is estimated to include some 1.2 million North Carolinians..

23. There are common questions of law and fact that exist as to all members of the Nationwide Class and the North Carolina Subclass. Such questions predominate over any question affecting only an individual Nationwide Class or Subclass member. Those common questions include, but are not limited to:

a. Whether Target failed to use reasonable care and utilize commercially reasonable methods to secure and safeguard its customers' sensitive personal and financial data;

b. Whether Target unreasonably delayed informing customers of the security breach and in taking appropriate steps to remedy the loss of service and impact of the breach;

c. Whether Target's conduct violated the Federal Stored Communications Act, 18 U.S.C. § 2702; and

d. Whether Plaintiff and the Class have been damaged as a result of Target's actions and, if so, what is the appropriate measure of relief.

24. There are common questions of law and fact that exist as to all members the North Carolina Subclass. Such questions predominate over any question affecting only an individual Subclass member. Those common questions include, but are not limited to:

a. Whether Target, through its conduct, has violated Chapter 75 of the North Carolina General Statutes by engaging in an unfair and deceptive trade practice; and

b. The proper measure of damages for the Subclass.

25. Plaintiff's claims are typical of the claims of the proposed Class. Each Class and Subclass member was subjected to the same unlawful and negligent conduct, suffered the same breach of their credit or debit card information and personal information, and therefore has the same claims.

26. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained counsel competent and experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of the Class members will be fairly and adequately protected by Plaintiff and his counsel.

27. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecutions of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Additionally, individualized

litigation presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I (ALL CLASS MEMBERS)

Violation of the Federal Stored Communications Act, 18 U.S.C. § 2702

28. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of the Complaint.

29. The Stored Communications Act ("SCA") provides consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3557.

30. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

31. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Id. at § 2510(15).

32. Through its payment processing equipment (including its PIN pad terminals), Target provides an "electronic communication service to the public" within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability

that enables consumers to send or receive wire or electronic communications concerning their account data to transaction managers, card companies or banks.

33. By failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Target has knowingly divulged customer credit and debit card account information that were communicated to financial institutions solely for customers' payment verification purposes, while in electronic storage in TARGET's point-of-sale payment machines.

34. Section 2702(a)(2)(A) of the SCA provides "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

35. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

36. An "electronic communications system" is defined by the SCA as "any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

37. In addition to providing an electronic communications service, Target provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo-optical or

photoelectric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer financial information for the electronic storage of such communications during the payment verification process.

38. By failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Target has knowingly divulged customer credit and debit card account information that was carried and maintained on TARGET's remote computing service solely for the customer's payment verification purposes.

39. As a result of Target's conduct described herein and its violations of § 2702(a)(1) and (2)(A), Plaintiff and the Class have suffered damages, including the loss of their money, losses associated with the inability to access funds to which they were entitled, and costs associated with the need for vigilant credit monitoring and/or identity theft protection services to protect against additional identity theft. Accordingly, Plaintiff and the Class seek an order awarding the maximum statutory damages available under 18 U.S.C. § 2707, in addition to the cost for 3 years of credit monitoring and identity theft protection services.

COUNT II (ALL CLASS MEMBERS)

Negligence

40. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of the Complaint.

41. As a major national retailer that produced more than $72 billion in sales in 2012, much of which was transacted through the use of credit and debit cards, Target owed its customers a duty of care in the handling and safeguarding of their private and confidential financial and personal information entrusted to them for the purpose of making purchases at its stores.

42. Target, in coming into possession of Plaintiff and Class members' financial and personal information and agreeing to accept that financial and personal information through its payment processing services, assumed a duty to exercise reasonable care in safeguarding and protecting such information from being stolen, compromised, or improperly disclosed to third parties.

43. Target breached its duty of care by failing to provide adequate security, and failing to protect Plaintiff's and Class members' financial data and personal information from being captured, accessed, disseminated, and misused by a third party.

44. Target also had a duty to timely notify Plaintiffs and the Class members if their credit and debit card information or other personal or financial information had been compromised or improperly furnished to unauthorized third parties.

45. Target breached its duty of care by failing to provide prompt and clear notification to Plaintiff and members of the Class that their financial data and personal information had been compromised.

46. As a direct and proximate result of Target's failure to exercise reasonable care and use commercially reasonable security measures, Target subjected Plaintiff and other Class members to identity theft, and Plaintiff's and Class members' financial and personal information and bank account monies were, in fact, stolen. Plaintiff and Class members have suffered damages, including the theft of money as a result of fraudulent purchases, losses associated with the inability to access funds to which they were entitled, the theft of sensitive financial and personal information, and other damages associated with increased risk of identity theft.

47. Plaintiff and members of the Class have suffered injury in fact, including money damages, and will continue to incur damages as a result such negligence.

COUNT III (NORTH CAROLINA SUBCLASS)

Unfair and Deceptive Trade Practices

48. N.C. Gen. Stat. § 75-1.1 states that "unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." N.C. Gen. Stat. § 75-1.1(a).

49. "Commerce" includes all business activities, however denominated. N.C. Gen. Stat. § 75-1.1(b).

50. N.C. Gen. Stat. § 75-16 provides a right of action for individuals harmed by unfair or deceptive acts or practices in or affecting commerce.

51. A prevailing plaintiff is entitled to treble damages for violations of Chapter 75. See N.C. Gen. Stat. § 75-16.

52. The failure of Target to adequately and reasonably secure customers' private financial information and personal information, allowing for that information to be obtained by unauthorized third parties, constitutes an unfair or deceptive act or practice in or affecting commerce.

53. Further, N.C. Gen. Stat. § 75-65 states that entities that possess (but do not own or license) personal information must *immediately* notify the owner of that information when there has been a security breach. Specifically, N.C. Gen. Stat. § 75-65 provides that:

> Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of an security breach immediately following discovery of the breach consistent with the legitimate needs of law enforcement . . . .

N.C. Gen. Stat. § 75-65(b) (emphasis added).

54. "A violation of this section [§ 75-65] is a violation of G.S. 75-1.1." N.C. Gen. Stat. § 75-65(i).

55. Target does not own or license customers' personal financial information such as debit and credit card information and PIN numbers. Further, Target did not immediately notify customers, such as Plaintiff and other Subclass members, of the security breach when it discovered the breach on December 15, and therefore is in violation of N.C. Gen. Stat. § 75-65.

56. As a result of Defendant Target's unfair and deceptive trade practices and violations of Chapter 75 of the North Carolina General Statutes, Plaintiff and the members of the Subclass have and will continue to suffer injury. Accordingly, Plaintiff and the Subclass seeks damages for these injuries, trebled pursuant to N.C. Gen. Stat. § 75-16, together with all attorneys' fees, interest, and other recoverable costs as allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and members of the proposed Class, prays for:

1. All forms of relief set forth above;
2. An order certifying the proposed Class and appointing Plaintiffs and their undersigned counsel of record to represent the proposed Class;
3. Restitution and disgorgement of all amounts obtained by Defendant as a result of its misconduct;
4. Actual damages;
5. Compensatory damages;
6. Statutory damages;
7. An order requiring Defendant to immediately cease its wrongful conduct;
8. Punitive damages;

9. Cost of suit herein;

10. Both pre-judgment and post-judgment interest on any amounts awarded;

11. Payment of reasonable attorney's fees; and

12. Such other relief as this Court deems just and proper.

This the 17th day of January, 2014.

Respectfully submitted,

/s/ Gary W. Jackson
Gary W. Jackson
gjackson@ncadvocates.com
NC Bar #13976
Attorneys for Plaintiffs
The Jackson Law Group, PLLC
225 E. Worthington Ave., Ste. 200
Charlotte, NC 28203
Phone: (704) 377-6680
Fax: (704) 377-6690

/s/ Charles H. Rabon, Jr.
Charles H. Rabon, Jr.
NC State Bar No. 16800
CRabon@usfraudattorneys.com

/s/ Marshall P. Walker
Marshall P. Walker
NC State Bar No. 45040
mwalker@usfraudattorneys.com

Rabon Law Firm, PLLC
225 E. Worthington Avenue
Suite 100
Charlotte, NC 28203
Tel. 704-247-3247
Fax 704-208-4645